CoNe Freiburg

Peer-to-Peer Networks

Anonymity (1st part)

8th Week

Albert-Ludwigs-Universität Freiburg
Department of Computer Science
Computer Networks and Telematics
Christian Schindelhauer
Summer 2008

Motivation

- **Society**
  - Free speech is only possible if the speaker does not suffer negative consequences
  - Thus, only an anonymous speaker has truly free speech
- **Copyright infringement**
  - Copying items is the best (and most) a computer can do
  - Copyright laws restrict copying
  - Users of file sharing systems do not want to be penalized for their participation or behavior
- **Dictatorships**
  - A prerequisite for any oppressing system is the control of information and opinions
  - Authors, journalists, civil rights activists like all citizens should be able to openly publish documents without the fear of penalty
- **Democracies**
  - In many democratic states certain statements or documents are illegitimate, e.g.
    - (anti-) religious statements
    - insults (against the royalty)
    - certain sexual contents
    - political statements (e.g. for fascism, communism, separation, revolution)
- **A anonymizing P2P network should secure the privacy and anonymity of each user without endangering other users**

Terms

- **From**
  - Danezis, Diaz, A Survey of Anonymous Communication Channels
  - Pfitzmann, Hansen, Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology
- **Anonymity** (Pfitzmann-Hansen 2001)
  - describes the state of being not identifiable within a larger set of subjects (peers), i.e.
    - the anonymity set
  - The anonymity set can be all peers of a peer-to-peer network
    - yet can be another (smaller or larger) set

Terms

- **Unlinkability**
  - Absolute (ISO15408)
    - „ensures that a user may make multiple uses of resources or services without other being able to link these uses together.“
  - Relative
    - Any attacker cannot find out more about the connections of the uses by observing the system
      - a-priori knowledge = a-posteriori knowledge

Terms

- **Unobservability**
  - The items of interests are protected
  - The use or non-use of any service cannot be detected by an observer (attacker)
- **Pseudonymity**
  - is the use of pseudonyms as IDs
  - preserves accountability and trustability while preserving anonymity

Peer-to-Peer-Networks with Anonymity

- **Freenet**
  - 2000: Clarke, Oskar Sandberg, Brandon Wiley, Theodore Hong
- **FreeHaven**
  - 2000: Dingledine, Michael Freedman, David Molnar, Brian Sniffen und Todd Kamin
- **aChord**
  - 2002: Hazel, Wiley
- **GnuNet**
  - 2003: Bennett, Grothoff

Peer-to-Peer Networks

Cryptography in a Nutshell

Steganography

- **is the art and science to secretly store information or transmit information**
- **Goals**
  - hide messages
  - check originality or source
- **Examples**
  - small, invisible changes of pictures, audio-files, videos
  - e.g. change of the the least significant bit
  - micro-dots
- **Advantages**
  - the transmission of data is completely hidden
- **Disadvantages**
  - considerable overhead
  - e.g. 0.5% hidden data if the least significant bit of audio transmission is used
- **Caution!**
  - adding a file into an ignored area of another file is NOT steganography
    - e.g. add file to zip-file, jpg-file, etc.
  - since this tampering can be easily discovered

Symmetric Cryptography

- **This is the classic cryptography**
  - and only known way up to the 1960s
- **Components:**
  - Secret key S
  - Document T
  - Encryption function f:
    - encrypts document T to code C using key S:
    - C = f(S,T)
  - Decryption function g:
    - decrypts code C to document T using key S
    - T = f(S,C)
- **It is important that the secret key is only known by the sender and receiver**
- **Examples:**
  - Ceasar‘s code
  - Enigma
  - DES (digital encryption standard)
  - AES (advanced encryption standard)
- **If P = NP then all symmetric (pol.-computable) codes can be broken**
  - since this question is open, there is no provable secure cryptographic function
  - yet some encoding systems can be broken (e.g. Ceasar or Enigma)

Public-Key Cryptography

- **Developed by**
  - Diffie, Hellman, Rivest, Shamir, Adleman
- **Components:**
  - Secret key S
    - known only to the receiver of a message
  - Public key P
    - known to everybody
  - Document T
  - Encryption function f:
    - encrypts document T to code C using public key P:
    - **C = f(P,T)**
    - everybody can compute this function
  - Decryption function g:
    - decrypts code C to document T using secret key S
    - **T = g(S,C)**
- **It is important that the secret key is only known by the receiver**
- **Examples:**
  - RSA
  - El-Gamal
- **If P = NP then all such codes can be broken**
  - again no provable secure public-key cryptographic systems, only candiates

Rivest, Shamir, Adleman

- **Secret key:**
  - two large prime numbers p and q, and a number $d < pq$ which is no multiple of p or q
- **Public key**
  - product $n = p\,q$
  - $e = d^{-1} \bmod (p-1)(q-1)$
- **Message M**
  - is interpreted as number $M<n$ which is no multiple of p and q
  - for this, longer messages can be partitioned in to a series of smaller messages
  - a fixed offset can be added to each message, then the case of $p|M$ (p divides M) or $q|M$ occurs with extremely small probability
- **Encoding function f:**
  - $C = T^e \bmod n$
- **Decoding function g:**
  - $T = C^d \bmod n$
- **Computation is correct because of Euler‘s Theorem**
  - $x^{\varphi(n)} \bmod n = 1$, if $\gcd(x,n) = 1$
  - Euler‘s totient function $\varphi(n) = (p_1-1)\, p_1^{e_1-1} \ldots (p_k-1)\, p_k^{e_k-1\ e_k}$
    - if $n= p_1^{e_1}\, p_2^{e_2} \ldots p_k^{e_k}$ for prime numbers $p_1, p_2, \ldots, p_k$

Elgamal Code

- **Private key**
  - random exponent $x \in \{0,...,p-1\}$
- **Public key**
  - prime number p
  - a generator g
  - $h = g^x \bmod p$
- **Message T**
  - is in the set {2,..., p-1}
- **Encryption**
  - choose random number y
  - compute $c_1 = g^y \bmod p$
  - compute $c_2 = h^y T \bmod p$
  - publish (c_1,c_2)
- **Decoding function g:**

$$T = \frac{c_2}{(c_1)^x}$$

- **Security**
  - depends on the in-feasibility of computing the discrete logarithm module a prime number

Electronic Signatures

- **Given a message T**
- **The signer produces compressed text K**
  - K = h(T)
  - using a cryptographic secure hash function, like
    - MD5, SHA-1, SHA-2
  - computes signature G = g(S,K) using his secret key S
  - T, h, and public key P corresponding to S are published
- **Every user can check**
  - h(T) = K = f(P,G)

- **This is only an example of an electronic signature**
  - under certain attacks such codes can fail,
  - e.g. when used with RSA, if the signer does not create new keys
- **There are yet unbroken electronic signature schemes at hand,**
  - e.g. Goldwasser, Micali, Rivest „An signature scheme secure against adaptive chosen message attack“

Usability of Encrypted Data

- **Peers may store encrypted files**
  - the peer does not know the original text
  - the file is encrypted by the author
- **In addition the file may be signed**
  - for pseudonomity
  - only the author can change or revoke files
- **A reader may read the file**
  - when the authors commits his secret key (on a different path)
  - or the peer looking up the information can deduct this secret key from his search key
    - the author remains safe
- **Advantage**
  - the storage peer cannot be convicted for the contents he stores
- **Disadvantage**
  - the storage peer may possess fake data
    - to delete or not delete

Peer-to-Peer Networks

End of 8th Week

Albert-Ludwigs-Universität Freiburg
Department of Computer Science
Computer Networks and Telematics
Christian Schindelhauer
Summer 2008